

PATENT ABSTRACTS OF JAPAN

(1)Publication number : 11-282982

(43)Date of publication of application : 15.10.1999

(51)IntCl

G06K 17/00
G06F 15/00
G06K 19/10
G06K 19/073
G09C 1/00
H04L 9/10
H04L 9/32

(21)Application number : 10-085536

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 31.03.1998

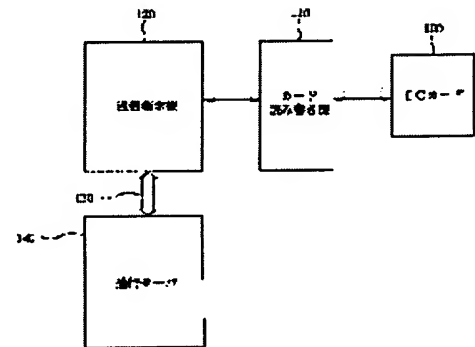
(72)Inventor : NISHIYAMA YOSHITAKA

(54) USER CARD, COMMUNICATION TERMINAL EQUIPMENT, COMMUNICATION SERVER, COMMUNICATION SYSTEM AND USER AUTHENTICATION METHOD FOR COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a user authentication method of a communication system capable of simplifying the operation of a user and simultaneously authenticating both of the user and a terminal equipment.

SOLUTION: When the user inputs a password for a card to the terminal equipment 120, the terminal equipment 120 transmits a connection request including a terminal equipment ID to a communication network 130 and a server 140 confirms the validity/invalidity of the terminal equipment 120 from the terminal equipment ID and then returns a challenge. Then, the terminal equipment 120 calculates a one-time password by using a seed inside the challenge, a password number and a terminal password and sends it to an IC card 100 together with the password for the card and a random number. The IC card 100 checks the password for the card, then ciphers data including the one-time password and the random number and sends them through the terminal equipment 120 to the server 140. The server 140 deciphers the received data and then, checks the terminal password, the random number and the one-time password.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-282982

(43) 公開日 平成11年(1999)10月15日

(51) Int.Cl.*	識別記号	F I	
G 0 6 K 17/00		G 0 6 K 17/00	T
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 G
			3 3 0 E
G 0 6 K 19/10		G 0 9 C 1/00	6 6 0 A
19/073		G 0 6 K 19/00	R

審査請求 未請求 請求項の数17 O L (全 12 頁) 最終頁に続く

(21) 出願番号 特願平10-85536

(22) 出願日 平成10年(1998)3月31日

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 西山 由高

東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内

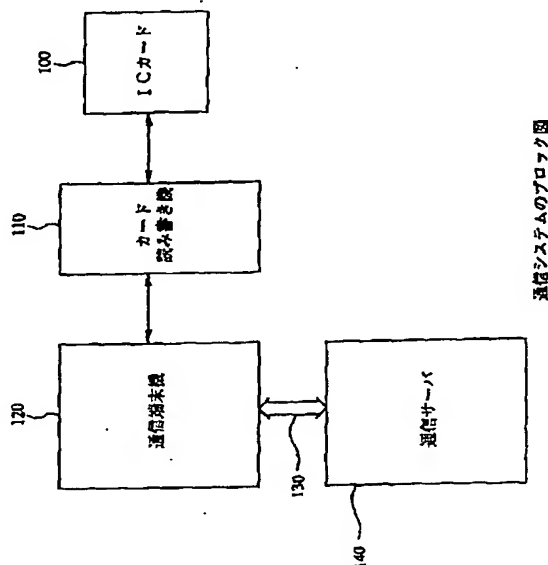
(74) 代理人 弁理士 大垣 孝

(54) 【発明の名称】 利用者カード、通信端末機、通信サーバ、通信システム、および、通信システムの利用者認証方法

(57) 【要約】

【課題】 利用者の操作が簡単で、且つ、利用者と端末機の認証とを両方同時に行うことができる、通信システムの利用者認証方法を提供する。

【解決手段】 端末機120に利用者がカード用パスワードを入力すると、この端末機120が端末機IDを含む接続要求を通信網130に送信し、サーバ140が端末機IDから端末機120の有効/無効を確認した後、チャレンジを返信する。続いて、端末機120が、チャレンジ内のシードおよびパスワード番号と端末パスワードとを用いてワンタイム・パスワードを算出し、カード用パスワードおよび乱数とともにICカード100に送る。ICカード100は、カード用パスワードをチャックした後、ワンタイム・パスワードと乱数とを含むデータを暗号化し、端末機120を介してサーバ140に送る。サーバ140は、受信したデータを復号化した後、端末パスワード、乱数およびワンタイム・パスワードのチェックを行う。



【特許請求の範囲】

【請求項1】 利用者が通信網を介して通信端末機と通信サーバとを接続するときの認証を行うための利用者カードであって、

利用者ID格納領域、カード用パスワード格納領域および秘密鍵格納領域を有する記憶手段と、外部からカード用パスワードおよび暗号用データを入力し、前記カード用パスワードが前記カード用パスワード格納領域から読み出したパスワードと一致する場合に、前記利用者ID記憶領域から読み出した利用者IDと前記暗号用データとを連結してなるデータを前記秘密鍵格納領域から読み出した秘密鍵を用いての利用者認証方法暗号化することによりカード暗号文を生成し、このカード暗号文を外部に出力する暗号化手段と、を備えたことを特徴とする利用者カード。

【請求項2】 前記記憶手段が前記利用者カード内に設けられた不揮発性メモリであることを特徴とする請求項1に記載の利用者カード。

【請求項3】 外部からのカード用パスワードおよび暗号用データの入力と、外部へのカード暗号文の出力とが、カード読み書き装置によって行われることを特徴とする請求項1または2に記載の利用者カード。

【請求項4】 利用者が通信網を介して通信サーバと接続するとき利用カードを用いて認証を行うための通信端末機であって、

端末機ID格納領域および端末機用パスワード格納領域を有する記憶手段と、

端末機IDを含む接続要求を前記通信網に送信するとともに、シードとパスワード番号と乱数とを含むチャレンジとを前記通信網から受信するチャレンジ要求手段と、このチャレンジ要求機能部から取り込んだ前記シードおよび前記パスワード番号と、前記端末機用パスワード格納領域から取り込んだ端末機用パスワードとを用いてワンタイム・パスワードを算出するパスワード生成手段と、

このパスワード生成手段から取り込んだ前記ワンタイムパスワードと前記チャレンジ要求手段から取り込んだ前記乱数とを連結して暗号用データを作成し、この暗号用データと利用者が入力したカード用パスワードとを前記利用者カードに送信するとともに、この利用者カードからカード暗号文を受信する暗号化要求手段と、この暗号化要求手段から取り込んだ前記カード暗号文を前記通信網に送信するとともに、この通信網から認証結果を受信する認証要求手段と、を備えたことを特徴とする通信端末機。

【請求項5】 前記利用者カードへの前記暗号用データおよび前記カード用パスワードの送信と、前記利用者カードからの前記カード暗号文の受信とが、カード読み書き装置を介して行われることを特徴とする請求項4に記載の通信端末機。

【請求項6】 通信網を介して通信端末機と接続するとき利用カードを用いて認証を行う通信サーバであって、

シードを記憶するシード記憶手段と、秘密鍵を記憶する秘密鍵記憶手段と、端末機ID、端末機有効/無効情報、パスワード番号および前回の認証時に使用されたワンタイム・パスワードを全ての登録通信端末機について記憶する端末機表と、利用者IDおよび利用者カード有効/無効情報を全ての登録利用者について記憶する利用者カード表と、端末機IDを含む接続要求を前記通信網から受信したときに、この端末機IDに対応する端末機有効/無効情報を前記端末機表から読み出し、この端末機有効/無効情報が有効である場合に、前記シード記憶手段から読み出した前記シードと前記端末機表から読み出した前記パスワード番号と新たに生成した乱数とからなるチャレンジを前記通信網に送信するチャレンジ生成手段と、カード暗号文を受信し、前記秘密鍵記憶手段から読み出した前記秘密鍵で前記カード暗号文を解読することにより利用者IDと乱数とワンタイム・パスワードとを取得し、この利用者IDに対応する前記利用者カード有効/無効情報の有効/無効と、この乱数と前記チャレンジとして送信した前記乱数との一致/不一致とを検証するカード暗号文検証手段と、

このカード暗号文検証手段が取得したワンタイム・パスワードを用いて前回の認証で使用されたワンタイム・パスワードを算出した後、このワンタイム・パスワードを前記端末機表から読み出した前記ワンタイム・パスワードと比較し、両者が一致する場合に、前記カード暗号文検証手段が取得したワンタイム・パスワードを前記端末機表に格納するとともに、この端末機表に記憶されている前記パスワード番号の値を「1」だけ増加させるパスワード検証手段と、を備えたことを特徴とする通信サーバ。

【請求項7】 前記利用者カードが有効で且つ前記乱数が一致すると前記カード暗号文検証手段が判断し、前記パスワードが一致すると前記パスワード認証手段が判断した場合に、前記通信網に認証応答を出力する認証手段をさらに備えたことを特徴とする請求項6に記載の通信サーバ。

【請求項8】 前記端末機が無効であると前記チャレンジ生成手段が判断した場合、前記利用者カードが無効或いは前記乱数が一致しないと前記カード暗号文検証手段が判断した場合または前記パスワードが一致しないと前記パスワード認証手段が判断した場合に、前記通信端末機との接続を切断することを特徴とする請求項6または7に記載の通信サーバ。

【請求項9】 接続時に認証を行う通信システムであって、

利用者ID格納領域、カード用パスワード格納領域およ

び秘密鍵格納領域を有するカード用記憶手段と、外部からカード用パスワードおよび暗号用データを入力し、前記カード用パスワードが前記カード用パスワード格納領域から読み出したパスワードと一致する場合に、前記利用者ID格納領域から読み出した利用者IDと前記暗号用データとを連結してなるデータを前記秘密鍵格納領域から読み出した秘密鍵を用いて暗号化することによりカード暗号文を生成し、このカード暗号文を外部に出力する暗号化手段とを備えた利用者カードと、
 端末機ID格納領域および端末機用パスワード格納領域を有する端末機用記憶手段と、端末機IDを含む接続要求を前記通信網に送信するとともに、シードとパスワード番号と乱数とを含むチャレンジとを前記通信網から受信するチャレンジ要求手段と、このチャレンジ要求機能部から取り込んだ前記シードおよび前記パスワード番号と、前記端末機用パスワード格納領域から取り込んだ端末機用パスワードとを用いてワンタイム・パスワードを算出する端末パスワード生成手段と、このパスワード生成手段から取り込んだ前記ワンタイム・パスワードと前記チャレンジ要求手段から取り込んだ前記乱数とを連結して暗号用データを作成し、この暗号用データと利用者が入力したカード用パスワードとを前記利用者カードに送信するとともに、この利用者カードからカード暗号文を受信する暗号化要求手段と、この暗号化要求手段から取り込んだ前記カード暗号文を前記通信網に送信するとともに、この通信網から認証結果を受信する認証要求手段とを備えた通信端末機と、
 シードを記憶するシード記憶手段と、秘密鍵を記憶する秘密鍵記憶手段と、端末機ID、端末機有効/無効情報、パスワード番号および前回の認証時に使用されたワンタイム・パスワードを全ての登録通信端末機について記憶する端末機表と、利用者IDおよび利用者カード有効/無効情報を全ての登録利用者について記憶する利用者カード表と、端末機IDを含む接続要求を前記通信網から受信したときに、この端末機IDに対応する端末機有効/無効情報を前記端末機表から読み出し、この端末機有効/無効情報が有効である場合に、前記シード記憶手段から読み出した前記シードと前記端末機表から読み出した前記パスワード番号と新たに生成した乱数とからなるチャレンジを前記通信網に送信するチャレンジ生成手段と、カード暗号文を受信し、前記秘密鍵記憶手段から読み出した前記秘密鍵で前記カード暗号文を解読することにより利用者IDと乱数とワンタイム・パスワードとを取得し、この利用者IDに対応する前記利用者カード有効/無効情報の有効/無効と、この乱数と前記チャレンジとして送信した前記乱数との一致/不一致とを検証するカード暗号文検証手段と、このカード暗号文検証手段が取得したワンタイム・パスワードを用いて前回の認証で使用されたワンタイム・パスワードを算出した後、このワンタイム・パスワードを前記端末機表から読

み出した前記ワンタイム・パスワードと比較し、両者が一致する場合に、前記カード暗号文検証手段が取得したワンタイム・パスワードを前記端末機表に格納するとともに、この端末機表に記憶されている前記パスワード番号の値を「1」だけ増加させるパスワード検証手段とを備えた通信サーバと、
 を有することを特徴とする通信システム。

【請求項10】 前記カード用記憶手段が前記利用者カード内に設けられた不揮発性メモリであることを特徴とする請求項9に記載の通信システム。

【請求項11】 外部から利用者カードへのカード用パスワードおよび暗号用データの入力と、利用者カードから外部へのカード暗号文の出力とが、カード読み書き装置によって行われることを特徴とする請求項9または10に記載の通信システム。

【請求項12】 前記利用者カードが有効で且つ前記乱数が一致すると前記カード暗号文検証手段が判断し、前記パスワードが一致すると前記パスワード認証手段が判断した場合に、前記通信網に認証応答を出力する認証手段をさらに備えたことを特徴とする請求項9～11のいずれかに記載の通信システム。

【請求項13】 前記端末機が無効であると前記チャレンジ生成手段が判断した場合、前記利用者カードが無効或いは前記乱数が一致しないと前記カード暗号文検証手段が判断した場合または前記パスワードが一致しないと前記パスワード認証手段が判断した場合に、前記通信サーバが前記通信端末機との接続を切断することを特徴とする請求項9～12のいずれかに記載の通信システム。

【請求項14】 通信網を介して通信端末機と通信サーバとを接続したときに利用者および通信端末機を認証するための、通信システムの利用者認証方法であって、通信端末機が、端末機IDを含む接続要求を前記通信網に送信する第1過程と、
 通信サーバが、前記通信網から前記接続要求を受信して、この接続要求内の前記端末機IDに対応する端末機有効/無効情報が有効である場合に、シード記憶手段に記憶されたシードと端末機表に記憶されたパスワード番号と新たに生成した乱数とからなるチャレンジを前記通信網に送信する第2過程と、

前記通信端末機が、前記チャレンジを前記通信網から受信し、このチャレンジ内の前記シードおよび前記パスワード番号と端末機用パスワードとを用いてワンタイム・パスワードを算出する第3過程と、
 前記ワンタイム・パスワードと前記乱数とを連結して暗号用データを作成し、利用者が入力したカード用パスワードとともに、前記通信端末機から利用者カードに転送する第4過程と、
 前記利用者カードが、前記カード用パスワードがパスワード格納領域に記憶されたパスワードと一致する場合に、利用者ID格納領域に記憶された利用者IDと前記

暗号用データとを連結してなるデータを秘密鍵で暗号化することによりカード暗号文を生成し、このカード暗号文を前記通信端末機に送信する第5過程と、前記通信端末機が前記カード用暗号文を前記通信網に転送する第6過程と、

前記通信サーバが、前記通信網から受信した前記カード用暗号文を秘密鍵で解読することにより利用者IDと乱数とワнтаイム・パスワードとを取得し、この利用者IDに対応する利用者カード有効/無効情報の有効/無効と、この乱数と前記チャレンジとして送信した前記乱数との一致/不一致とを検証する第7過程と、

前記カード用暗号文を解読して得られた前記ワнтаイム・パスワードを用いて前回の認証で使用されたワнтаイム・パスワードを算出した後、このワнтаイム・パスワードを前記端末機表に記憶された前回の認証で実際に使用されたワнтаイム・パスワードと比較し、両者が一致する場合に、前記カード用暗号文を解読して得られた前記ワнтаイム・パスワードを前記端末機表に格納するとともに、この端末機表に記憶されている前記パスワード番号の値を「1」だけ増加させる第8過程と、を有することを特徴とする通信システムの利用者認証方法。

【請求項15】 外部からのカード用パスワードおよび暗号用データの入力と、外部へのカード暗号文の出力とが、カード読み書き装置によって行われることを特徴とする請求項14に記載の通信システムの利用者認証方法。

【請求項16】 前記利用者カードが有効で且つ前記乱数が一致すると前記第7過程で判断され、前記パスワードが一致すると前記第8過程で判断された場合に、前記通信サーバが前記通信網に認証応答を出力することを特徴とする請求項14または15に記載の通信システムの利用者認証方法。

【請求項17】 前記端末機が無効であると前記第2過程で判断された場合、前記利用者カードが無効或いは前記乱数が一致しないと前記第7過程で判断され場合または前記パスワードが一致しないと前記第8過程で判断された場合に、前記通信サーバが前記通信端末機との接続を切断することを特徴とする請求項14～17のいずれかに記載の通信システムの利用者認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、通信網を介して通信端末機と通信サーバとを接続したときに利用者の正当性を検証する技術に関するものである。

【0002】

【従来の技術】通信網を介して通信端末機と通信サーバとを接続したときには、利用者が接続の権利を有するものであるか否かを確認する必要がある。

【0003】従来の通信網では、この確認は、利用者

が、通信端末を用いて利用者IDとパスワードとを通信サーバに送信することによって、行われていた。

【0004】このため、他人が利用者からパスワードを盗んで通信網を不正に使用しないための防護策が、必要であった。

【0005】従来は、パスワードの盗難を防止するために、利用者がパスワードを適宜変更することを可能にしていた。しかし、この方法では、実際には、同一のパスワードが多数回にわたって使用されることが多い。また、一般には、利用者は、盗難が発生したことをすぐには気づかない場合が多い。このため、利用者のパスワードが他人に盗まれた場合には、この利用者がパスワードを変更するまでの間、パスワードを盗んだ他人の不正使用を許してしまうこととなる。

【0006】パスワードの盗難は、利用者がパスワードの入力作業を他人に見られた場合や、他人が管理する通信端末機等を使用して通信サーバに接続する場合や、ネットワーク上でパスワードをコピーされた場合などに、発生する。

【0007】これに対して、他人の不正使用を防止できる利用者認証方法として、「ワнтаイム・パスワード」を用いた方法が提案されている。この方法を開示した文献としては、例えば、以下のようなものがある。

【0008】①稲村雄 “ワнтаイム・パスワード” 雑誌「オープンデザイン」No. 141996年6月号第30頁～第39頁 CQ出版社

②Ravi Kalakota and Andrew B. Whinston, “Token or Smart-Card Authentication”, Frontier of Electronic Commerce, p. 204, Addison-Wesley Publishing company, Inc., 1996.

このワнтаイム・パスワードを用いた場合、同一のパスワードは一回しか使用されないため、他人がパスワードを盗んで不正に使用することを有効に防止できる。

【0009】

【発明が解決しようとする課題】上述の文献に開示されているように、ワнтаイム・パスワード法では、ワнтаイム・パスワードを算出するための関数として、一方向関数 $F(x)$ を用いる。すなわち、このワнтаイム・パスワード法では、一方向関数 $F(x)$ を用いて、 $m-1$ 回目の認証作業で用いたワнтаイム・パスワードから m 回目の認証作業で用いるワнтаイム・パスワードを計算することが非常に困難で、且つ、 m 回目の認証作業で用いたワнтаイム・パスワードから $m-1$ 回目の認証作業で用いたワнтаイム・パスワードを計算することは簡単であるような、ワнтаイム・パスワード列を作成する。

【0010】ワнтаイム・パスワード生成プログラムは、信頼のおけるコンピュータ上で実行される。利用者は、まず、自分で任意に決定したパスワードとシード（そのサーバに固有の数値を示す文字列）とを、このコンピュータに入力する。

【0011】ワンタイム・パスワード生成プログラムは、このパスワードとシードとを連結して文字列 s を作成し、この s を用いた一方向関数 $F(s)$ の演算を実行する。この一方向関数としては、通信サーバによって定められた関数を使用され、例えばMD4、MD5、SHA1等が使用できる。ここでは、この演算の結果を P （すなわち $P_1 = F(s)$ ）とする。

【0012】続いて、ワンタイム・パスワード生成プログラムは、1回目の演算結果 P_1 を用いた一方向関数 $P_{1+1} = F(P_1)$ の演算を実行する。以下同様にして、前回の演算結果を用いた一方向関数の演算を繰り返し実行することにより、下記の演算結果 P_1, P_{1+1}, \dots, P_m を得る。これらの演算結果 P_1, P_{1+1}, \dots, P_m が、ワンタイム・パスワード列を構成する。

【0013】

$$P_1 = F(s)$$

$$P_{1+1} = F(P_1)$$

$$P_{1+2} = F(P_{1+1})$$

.

.

.

$$P_1 = F(P_1)$$

$$P_m = F(P_1)$$

次に、利用者が、通信端末機を用いて、利用者名と演算結果 P_m とを通信サーバに登録する。そして、利用者は、通信端末機を通信サーバに接続を行う度に、上述の演算結果 P_1, \dots, P_m を、ワンタイム・パスワードとして、 P_1 から順番に1個ずつ使用していく。

【0014】一方、通信サーバは、ワンタイム・パスワード P_1 を通信端末機から受信すると、このワンタイム・パスワード P_1 を用いて $P_m = F(P_1)$ を演算する。続いて、演算結果 P_m を、利用者によって先に登録された P_m と比較する。そして、両者が一致した場合は、ワンタイム・パスワード P_1 を次回の認証用データとして記憶するとともに、利用回数として「1」を記憶する。これと同様に、2回目以降の認証（ここでは m 回目とする）においても、通信サーバは、通信端末機から受信したワンタイム・パスワード P_m を用いて $P_{m+1} = F(P_m)$ を演算し、この演算結果を前回（すなわち $m-1$ 回目）のワンタイム・パスワードと比較することにより、利用者の認証を行うことができる。

【0015】上述したように、ワンタイム・パスワードの演算には、一方向関数 $F(x)$ を使用しているので、 m 回目のワンタイム・パスワード P_m から $m-1$ 回目のワンタイム・パスワード $P_{m-1} (= F(P_m))$ を算出することは容易であるが、 m 回目のワンタイム・パスワード P_m から $m+1$ 回目のワンタイム・パスワード P_{m+1} を算出することは困難である。従って、このワンタイム・パスワードを通信端末機から通信サーバに送信する際に他人に盗まれても、盗んだパスワードを用いて他人が通信

サーバに不正にログインすることは非常に困難である。また、利用者の秘密のパスワードを通信サーバに送信する必要はないので、この秘密のパスワードを他人に盗まれる可能性も少ない。

【0016】但し、上述のようにして算出したワンタイム・パスワード列 P_1, P_{1+1}, \dots, P_m をそのままコンピュータに記憶させておくと、このコンピュータから他人がワンタイム・パスワードを読み出して不正使用のおそれがある。このため、実際の運用上は、以下のようにして、接続作業のたびに、利用者がワンタイム・パスワードを算出する。

【0017】まず、利用者が利用者IDを通信端末機に入力し、この利用者IDと接続要求コードとを通信端末機から通信サーバに送信する。通信サーバは、これらの情報を受信すると、この利用者のパスワード利用回数を示すデータと上述のシードとを、通信端末機に送信する。これらの送信データ全体を「チャレンジ」と称する。なお、ここでは m 回目の接続を行う場合を例にとって説明する。このため、チャレンジに含まれる利用回数データは「 $m-1$ 」となる。

【0018】そして、利用者は、予め用意されたパスワード生成プログラムをコンピュータ上で実行する。このプログラムは、シードと利用者の秘密のパスワードとを用いて文字列 s を作成した後、上述の一方向関数 $P_1 = F(s), P_{1+1} = F(P_1), \dots, P_m = F(P_{m-1})$ の演算を順次実行する。これにより、今回の接続（すなわち m 回目の接続）で使用されるワンタイム・パスワード P_m を算出することができる。そして、このようにして生成されたワンタイム・パスワード P_m が、通信端末機から通信サーバに送信される。通信サーバは、ワンタイム・パスワードを受信すると、受信したワンタイム・パスワードから前回の接続（すなわち $m-1$ 回目の接続）で使用したワンタイム・パスワードを演算し、この演算結果をサーバ内に記憶された前回のワンタイム・パスワードと比較する。そして、両者が一致する場合に利用者を正当であると認証する。

【0019】なお、パスワード生成プログラムは、一般には通信端末機上で実行することができるが、携帯型のパスワード生成機を使用することも可能である。このパスワード生成機を利用することにより、パスワード生成プログラムを実行できない通信端末機で通信を行う場合にもワンタイム・パスワードによる認証方法を用いることができ、また、他人が管理する通信端末機等で通信を行う場合に上述の「利用者の秘密のパスワード」が盗まれることを防止できる。

【0020】このような方法によれば、同一のパスワードは一回しか使用されないで、利用者がパスワードの入力作業を他人に見られた場合や、ネットワーク上でパスワードをコピーされた場合でも、その他人による不正使用が発生するおそれが少ない。

【0021】しかしながら、ワンタイム・パスワード法には、使用者がチャレンジと秘密のパスワードとを用いて自分でワンタイム・パスワードを算出しなければならず、このため、接続時の操作が煩雑になるという欠点があった。また、上述のようなパスワード生成機を用いてワンタイム・パスワードを生成する場合には、このパスワード生成機を携帯していなければならず、この点でも利用者の負担が大きかった。

【0022】また、上述のような方法では、利用者の秘密のパスワードをネットワーク上で他人に盗まれるおそれはないものの、ワンタイム・パスワードの演算を行う際に他人に秘密のパスワードを盗まれた場合には、その他人が自分でワンタイム・パスワードを生成して不正使用を行うことが可能であり、不正使用の防止が不十分であった。

【0023】さらに、ワンタイム・パスワード法では、利用者の認証のみを行い、通信端末機の認証は行っていないので、偽造された通信端末機の使用を防止することができないという欠点があった。偽造された通信端末機を利用者に使用させることにより、例えば第三者が通信サーバから送られてきた情報をコピーして盗むなどの不正を行うことが可能となる。このような不正を防止するためには、通信端末機に対しても認証を行うことが望ましい。

【0024】加えて、通信サーバによって提供されるサービスの不正使用を防止するためには、利用できるサービスを利用者ごと或いは通信端末機ごとに制限することが望ましい場合がある。例えば、銀行における口座振替のサービスの場合であれば、ATM(Automatic Tellers Machine)の要に厳しい管理が行われている端末機では金額や利用回数を制限しないが、ホームバンキング用端末機のように厳しい管理が困難な端末機では1回の口座振替で許可する金額や1日の利用回数を制限するというように、通信端末機の機能や設置場所等に応じてサービス内容に差異を設けることが望ましい。このような点からも、通信サーバによる認証は、利用者と通信端末機との両方について行うことが望ましい。

【0025】このような理由から、利用者の操作が簡単で、且つ、利用者と通信端末機の認証とを両方行うことができる利用者認証方法が嚆望されていた。

【0026】

【課題を解決するための手段】

(1) 第1の発明は、利用者が通信網を介して通信端末機と通信サーバとを接続するときの認証を行うための利用者カードに関する。

【0027】そして、利用者ID格納領域、カード用パスワード格納領域および秘密鍵格納領域を有する記憶手段と、外部からカード用パスワードおよび暗号用データを入力し、カード用パスワードがカード用パスワード格納領域から読み出したパスワードと一致する場合に、利

用者ID格納領域から読み出した利用者IDと暗号用データとを連結してなるデータを秘密鍵格納領域から読み出した秘密鍵を用いて暗号化することによりカード暗号文を生成し、このカード暗号文を外部に出力する暗号化手段とを備える。

【0028】(2) 第2の発明は、利用者が通信網を介して通信サーバと接続するとき利用者カードを用いて認証を行うための通信端末機に関する。

【0029】そして、端末機ID格納領域および端末機用パスワード格納領域を有する記憶手段と、端末機IDを含む接続要求を通信網に送信するとともに、シードとパスワード番号と乱数とを含むチャレンジとを通信網から受信するチャレンジ要求手段と、このチャレンジ要求機能部から取り込んだシードおよびパスワード番号と、端末機用パスワード格納領域から取り込んだ端末機用パスワードとを用いてワンタイム・パスワードを算出する端末パスワード生成手段と、このパスワード生成手段から取り込んだワンタイム・パスワードとチャレンジ要求手段から取り込んだ乱数とを連結して暗号用データを作成し、この暗号用データと利用者が入力したカード用パスワードとを利用者カードに送信するとともに、この利用者カードからカード暗号文を受信する暗号化要求手段と、この暗号化要求手段から取り込んだカード暗号文を通信網に送信するとともに、この通信網から認証結果を受信する認証要求手段とを備える。

【0030】(3) 第3の発明は、通信網を介して通信端末機と接続するとき利用者カードを用いて認証を行う通信サーバに関する。

【0031】そして、シードを記憶するシード記憶手段と、秘密鍵を記憶する秘密鍵記憶手段と、端末機ID、端末機有効/無効情報、パスワード番号および前回の認証時に使用されたワンタイム・パスワードを全ての登録通信端末機について記憶する端末機表と、利用者IDおよび利用者カード有効/無効情報を全ての登録利用者について記憶する利用者カード表と、端末機IDを含む接続要求を通信網から受信したときに、この端末機IDに対応する端末機有効/無効情報を端末機表から読み出し、この端末機有効/無効情報が有効である場合に、シード記憶手段から読み出したシードと端末機表から読み出したパスワード番号と新たに生成した乱数とからなるチャレンジを通信網に送信するチャレンジ生成手段と、通信網からカード暗号文を受信し、秘密鍵記憶手段から読み出した秘密鍵でカード暗号文を解読することにより利用者IDと乱数とワンタイム・パスワードとを取得し、この利用者IDに対応する利用者カード有効/無効情報の有効/無効と、この乱数とチャレンジとして送信した乱数との一致/不一致とを検証するカード暗号文検証手段と、このカード暗号文検証手段が取得したワンタイム・パスワードを用いて前回の認証で使用されたワンタイム・パスワードを算出した後、このワンタイム・パ

パスワードを端末機表から読み出したワンタイム・パスワードと比較し、両者が一致する場合に、カード暗号文検証手段が取得したワンタイム・パスワードを端末機表に格納するとともに、この端末機表に記憶されているパスワード番号の値を「1」だけ増加させるパスワード検証手段とを備える。

【0032】(4)第4の発明は、接続時に認証を行う通信システムに関する。

【0033】そして、利用者ID格納領域、カード用パスワード格納領域および秘密鍵格納領域を有するカード用記憶手段と、外部からカード用パスワードおよび暗号用データを入力し、カード用パスワードがカード用パスワード格納領域から読み出したパスワードと一致する場合に、利用者ID格納領域から読み出した利用者IDと暗号用データとを連結してなるデータを秘密鍵格納領域から読み出した秘密鍵を用いて暗号化することによりカード暗号文を生成し、このカード暗号文を外部に出力する暗号化手段とを備えた利用者カードと、端末機ID格納領域および端末機用パスワード格納領域を有する端末機用記憶手段と、端末機IDを含む接続要求を通信網に送信するとともに、シードとパスワード番号と乱数とを含むチャレンジとを通信網から受信するチャレンジ要求手段と、このチャレンジ要求機能部から取り込んだシードおよびパスワード番号と、端末機用パスワード格納領域から取り込んだ端末機用パスワードとを用いてワンタイム・パスワードを算出する端末パスワード生成手段と、このパスワード生成手段から取り込んだワンタイム・パスワードとチャレンジ要求手段から取り込んだ乱数とを連結して暗号用データを作成し、この暗号用データと利用者が入力したカード用パスワードとを利用者カードに送信するとともに、この利用者カードからカード暗号文を受信する暗号化要求手段と、この暗号化要求手段から取り込んだカード暗号文を通信網に送信するとともに、この通信網から認証結果を受信する認証要求手段とを備えた通信端末機と、シードを記憶するシード記憶手段と、秘密鍵を記憶する秘密鍵記憶手段と、端末機ID、端末機有効／無効情報、パスワード番号および前回の認証時に使用されたワンタイム・パスワードを全ての登録通信端末機について記憶する端末機表と、利用者IDおよび利用者カード有効／無効情報を全ての登録利用者について記憶する利用者カード表と、端末機IDを含む接続要求を通信網から受信したときに、この端末機IDに対応する端末機有効／無効情報を端末機表から読み出し、この端末機有効／無効情報が有効である場合に、シード記憶手段から読み出したシードと端末機表から読み出したパスワード番号と新たに生成した乱数とからなるチャレンジを通信網に送信するチャレンジ生成手段と、通信網からカード暗号文を受信し、秘密鍵記憶手段から読み出した秘密鍵でカード暗号文を解読することにより利用者IDと乱数とワンタイム・パスワードとを取

得し、この利用者IDに対応する利用者カード有効／無効情報の有効／無効と、この乱数とチャレンジとして送信した乱数との一致／不一致とを検証するカード暗号文検証手段と、このカード暗号文検証手段が取得したワンタイム・パスワードを用いて前回の認証で使用されたワンタイム・パスワードを算出した後、このワンタイム・パスワードを端末機表から読み出したワンタイム・パスワードと比較し、両者が一致する場合に、カード暗号文検証手段が取得したワンタイム・パスワードを端末機表に格納するとともに、この端末機表に記憶されているパスワード番号の値を「1」だけ増加させるパスワード検証手段とを備えた通信サーバとを有する。

【0034】(5)第5の発明は、通信網を介して通信端末機と通信サーバとを接続したときに利用者および通信端末機を認証するための、通信システムの利用者認証方法に関する。

【0035】そして、通信端末機が、端末機IDを含む接続要求を通信網に送信する第1過程と、通信サーバが、通信網から接続要求を受信して、この接続要求内の端末機IDに対応する端末機有効／無効情報が有効である場合に、シード記憶手段に記憶されたシードと端末機表に記憶されたパスワード番号と新たに生成した乱数とからなるチャレンジを通信網に送信する第2過程と、通信端末機が、チャレンジを通信網から受信し、このチャレンジ内のシードおよびパスワードと端末機用パスワードとを用いてワンタイム・パスワードを算出する第3過程と、ワンタイム・パスワードと乱数とを連結して暗号用データを作成し、利用者が入力したカード用パスワードとともに、通信端末機から利用者カードに転送する第4過程と、利用者カードが、カード用パスワードがパスワード格納領域に記憶されたパスワードと一致する場合に、利用者ID格納領域に記憶された利用者IDと暗号用データとを連結してなるデータを秘密鍵で暗号化することによりカード暗号文を生成し、このカード暗号文を通信端末機に送信する第5過程と、通信端末機がカード用暗号文を通信網に転送する第6過程と、通信サーバが、通信網から受信したカード用暗号文を秘密鍵で解読することにより利用者IDと乱数とワンタイム・パスワードとを取得し、この利用者IDに対応する利用者カード有効／無効情報の有効／無効と、この乱数とチャレンジとして送信した乱数との一致／不一致とを検証する第7過程と、カード用暗号文を解読して得られたワンタイム・パスワードを用いて前回の認証で使用されたワンタイム・パスワードを算出した後、このワンタイム・パスワードを端末機表に記憶された前回の認証で実際に使用されたワンタイム・パスワードと比較し、両者が一致する場合に、カード用暗号文を解読して得られたワンタイム・パスワードを端末機表に格納するとともに、この端末機表に記憶されているパスワード番号の値を「1」だけ増加させる第8過程とを有する。

【0036】(6)この発明によれば、使用者が自分でワнтаイム・パスワードを算出する必要がないので、接続時の操作が簡単になり、パスワード生成機を携帯する必要もない。また、カード用パスワードは通信端末機を介して通信サーバに送信されないで、このカード用パスワードを外から不正に読み出すことはできず、従って、他人が利用者カードの不正使用を行うことは不可能である。さらに、通信サーバが利用者の認証と通信端末機の認証とを同時に行うことができる。

【0037】

【発明の実施の形態】以下、この発明の実施の形態について、図面を用いて説明する。なお、図中、各構成成分の大きさ、形状および配置関係は、この発明が理解できる程度に概略的に示してあるにすぎず、また、以下に説明する数値的条件は単なる例示にすぎないことを理解されたい。

【0038】図1は、この実施の形態に係る通信システムの全体構成を概略的に示すブロック図である。また、図2はICカードの内部構成を概略的に示すブロック図、図3は通信端末機の内部構成を概略的に示すブロック図、図4は通信サーバの内部構成を概略的に示すブロック図である。

【0039】図1において、利用者カードとしてのICカード100は、カード読み書き機110にセットされると、このカード読み書き機110を介して通信端末機120に接続される。また、通信端末機120は、通信網130を介して、通信サーバ140と接続される。

【0040】図2に示したICカード100において、利用者ID格納領域101にはこのICカード100の利用者名を示す情報である利用者ID(例えば10バイト長)が、カード用パスワード格納領域102にはこのICカードの利用者を認証するためのカード用パスワード(例えば8バイト長)が、秘密鍵格納領域103には所定データ(後述)を暗号化することによりカード暗号文を生成するための秘密鍵(例えばDES(Data Encryption Standard)方式のもの)が、それぞれ格納される。

【0041】また、暗号化機能部104は、後述のようにして、カード用パスワードのチェックと、カード暗号文の生成とを行う。

【0042】図3に示した通信端末機120において、端末機ID格納領域121にはこの通信端末機120を示す情報である端末機ID(例えば8バイト長)が、端末パスワード格納領域122にはこの通信端末機120を認証するための端末パスワード(例えば8バイト長)が、それぞれ格納される。

【0043】チャレンジ要求機能部123は、通信網130を介して通信サーバ140にチャレンジ要求を行うとともに、通信サーバ140からチャレンジ(シード、パスワード番号および乱数から構成される)を取得する。

【0044】パスワード生成機能部124は、後述するように、チャレンジ中のシードおよびパスワード番号と端末パスワード格納領域122から読み出した端末機パスワードとを用いてワнтаイム・パスワード(例えば8バイト長)を生成する。

【0045】暗号化要求機能部125は、パスワード生成機能部124が生成したワнтаイム・パスワードと、端末パスワード格納領域122から読み出した端末パスワードと、チャレンジ中の乱数とを連結してなるデータを、ICカード100の暗号化機能部104に送る。また、この暗号化機能部104からカード暗号文を受信する。

【0046】認証要求機能部126は、暗号化要求機能部125から取り込んだカード暗号文を通信網130に送信するとともに、この通信網130から認証結果を受信する。

【0047】図4に示した通信サーバ140において、シード格納領域141にはシード(そのサーバに固有の文字列)が、秘密鍵格納領域142には秘密鍵が、それぞれ記憶されている。

【0048】端末機表143は、端末機ID、端末機有効/無効情報、パスワード番号および前回の認証時に使用されたワнтаイム・パスワードを全ての登録通信端末機について記憶する。

【0049】ICカード表144は、利用者IDおよびICカード有効/無効情報を全ての登録利用者について記憶する。

【0050】チャレンジ生成機能部145は、通信端末機120のチャレンジ要求機能部123からチャレンジ要求を受信したときに、この通信端末機120の有効/無効の判断を行う。そして、この通信端末機120が有効である場合に、シード、パスワード番号および乱数からなるチャレンジを、チャレンジ要求機能部123に送信する。

【0051】カード暗号文検証機能部146は、後述の認証機能部148から入力したカード暗号文を秘密鍵で解読することにより利用者IDと乱数とワнтаイム・パスワードとを取得し、この利用者IDに対応する前記ICカード有効/無効情報の有効/無効と、この乱数と前記チャレンジとして送信した前記乱数との一致/不一致とを検証する。

【0052】パスワード検証機能部147は、カード暗号文検証機能部146から入力したワнтаイム・パスワードを用いて前回の認証で使用されたワнтаイム・パスワードを算出した後、このワнтаイム・パスワードを端末機表143から読み出したワнтаイム・パスワードと比較し、両者が一致する場合に、カード暗号文検証機能部146が取得したワнтаイム・パスワードを端末機表143に格納するとともに、この端末機表143に記憶されているパスワード番号の値を「1」だけ増加させ

10

20

30

40

50

る。

【0053】認証機能部148は、通信端末機120から受信したカード暗号文をカード暗号文検証機能部146に転送し、このカード暗号文検証機能部146から入力したワンタイム・パスワードをパスワード検証機能部147に転送し、さらに、このパスワード検証機能部147がワンタイム・パスワードが有効であると判断した場合に、通信網130に認証応答を送信する。

【0054】次に、図1～図4に示した通信システムの全体動作について説明する。

【0055】まず、利用者が、自分のICカード100をカード読み書き機110にセットする。これにより、このカード読み書き機110を介して、ICカード100と通信端末機120とが接続される。

【0056】続いて、利用者が、図示しない入力装置を用いて、通信端末機120の認証要求機能部126にカード用パスワードを入力する。

【0057】通信端末機120の認証要求機能部126は、利用者によってカード用パスワードが入力されると、チャレンジ要求機能部123を起動する。このチャレンジ要求機能部123は、端末機ID格納領域121から端末機IDを読み出して、この端末機IDを含むチャレンジ要求を通信網130に出力する。

【0058】このチャレンジ要求は、通信網130を介して、通信サーバ140のチャレンジ生成機能部145に受信される。チャレンジ生成機能部145は、チャレンジ要求を受信すると、まず、このチャレンジ要求に含まれる端末機IDに対応する端末機有効/無効情報を端末機表から読み出す。そして、この端末機有効/無効情報が「有効」である場合には、チャレンジ生成機能部145は、シード格納領域141からのシードの読み出しと端末機表143からのパスワード番号の読み出しとを行い、さらに、このチャレンジ生成機能部145内で乱数を生成する。その後、このチャレンジ生成機能部145は、かかるシード、パスワード番号および乱数からチャレンジを生成して、通信網130に出力する。一方、端末機有効/無効情報が「無効」である場合には、通信サーバ140は、所定の異常処理を行って回線を切断する。

【0059】チャレンジ要求機能部123は、通信網130からチャレンジを受信すると、このチャレンジに含まれるシード、パスワード番号および乱数を、認証要求機能部126に送る。

【0060】認証要求機能部126は、かかるシード、パスワード番号および乱数のうち、シードおよびパスワード番号を、パスワード生成機能部124に送る。

【0061】パスワード生成機能部124は、シードおよびパスワード番号（ここでは「m」とする）を受信すると、続いて、端末パスワード格納領域122から端末機パスワードを読み出す。そして、シードと端末パスワ

ードとを用いて文字列sを作成した後、従来と同様の一方方向関数 $P_i = F(s)$, $P_{i+1} = F(P_i)$, \dots , $P_n = F(P_{n-1})$ の演算を順次実行する。ここで、一方方向関数としては、従来と同様、例えばMD4, MD5, SHA1等が使用できる。さらに、パスワード生成機能部124は、演算結果 P_n （ここでは16バイトとする）の上位8バイトと下位8バイトの排他的論理和を演算する。そして、この演算の結果が、ワンタイム・パスワードとして、パスワード生成機能部124から認証要求機能部126に送られる。

【0062】認証要求機能部126は、このワンタイム・パスワードと、利用者が入力したカード用パスワード（上述）と、チャレンジ要求機能部123から受信した乱数（上述）とを、暗号化要求機能部125に送る。

【0063】暗号化要求機能部125は、ワンタイム・パスワードと乱数とを連結してなる暗号用データを生成し、この暗号用データをカード用パスワードとともにICカード読み書き機110に送信する。

【0064】図5に示したように、この送信データは、カード用パスワードに、ワンタイム・パスワードおよび乱数からなる暗号用データを連結することによって構成される。

【0065】ICカード100の暗号化機能部104は、ICカード読み書き機110を介して、暗号用データを受信する。そして、このカード用パスワードを、カード用パスワード格納領域102から読み出したカード用パスワードと比較する。そして、両者が一致する場合には、図6に示すようなデータを生成する。

【0066】図6に示したように、このデータは、開始コード、利用者ID、暗号用データおよび終了コードを連結することによって構成される。ここで、このデータの総バイト数は、秘密鍵のバイト数の整数倍にする必要がある。秘密鍵を8バイト長、利用者IDを10バイト長、暗号用データを16バイト長とした場合、開始コードと終了コードとの和は例えば6バイトとすればよい。例えば、開始コードを5バイト長（例えば16進数の4BBBBBBA）とし、終了コードを1バイト長（例えば16進数のBC）とすればよい。

【0067】続いて、暗号化機能部104は、秘密鍵格納領域103から秘密鍵を読み出し、この秘密鍵で上述のデータ（図6参照）を暗号化することによりカード暗号文を生成する。ここで、秘密鍵としては、例えばDES方式のCBCモードを使用することができる。その後、暗号化機能部104は、このカード暗号文をカード読み書き機110に出力する。

【0068】通信端末機120の暗号化要求機能部125は、カード読み書き機110からカード暗号文を受信して、認証要求機能部126に転送する。

【0069】認証要求機能部126は、暗号化要求機能部125から受信したカード暗号文を通信網130に出

10

20

30

40

50

力する。

【0070】通信サーバ140の認証機能部148は、通信網130からカード暗号文を受信し、このカード暗号文をカード暗号文検証機能部146に転送する。

【0071】カード暗号文検証機能部146は、秘密鍵格納領域142から秘密鍵を読み出し、この秘密鍵でカード暗号文を復号化することにより、図6に示したようなデータを得る。そして、開始コード（図6では16進数の4BBBBBA）および終了コード（図6では16進数のBC）が含まれているか否かをチェックする。そして、開始コードおよび終了コードが含まれていた場合には、このデータから利用者IDを抽出し、この利用者IDに対応するICカード有効/無効情報をICカード表144から読み出して、ICカードの有効/無効をチェックする。ここで、ICカードが有効であった場合には、乱数の値を、チャレンジ生成機能部145が送信したチャレンジに含まれていた乱数の値と比較する。そして、両者が一致した場合には、ワンタイム・パスワードを出力する。一方、ICカードが無効であった場合や乱数が一致しなかった場合は、所定の異常処理を行って回線を切断する。

【0072】パスワード検証機能部147は、認証機能部148を介してカード暗号文検証機能部146からワンタイム・パスワード（ここではP_iとする）を入力する。そして、一方関数 $P_{i+1} = F(P_i)$ を演算することによって前回の認証で使用されたワンタイム・パスワードP_iを算出した後、このワンタイム・パスワードP_iを端末機表143から読みだしたワンタイム・パスワードと比較し、両者が一致する場合に、カード暗号文検証機能部146が取得したワンタイム・パスワードP_iを端末機表143に格納するとともに、この端末機表143に記憶されているパスワード番号の値を「1」だけ増加させる。その後、認証機能部148から認証要求機能部126に認証結果が送信され、通信サーバ140と通信端末機120との間でログインのための処理が行われる。一方、これらのワンタイム・パスワードが一致しなかった場合には、所定の異常処理を行って回線を切断する。

【0073】このように、この実施の形態によれば、使用者が自分でワンタイム・パスワードを算出する必要がないので、接続時の操作が簡単になり、パスワード生成機を携帯する必要もない。

【0074】また、カード用パスワードは通信端末機120を介して通信サーバ140に送信されないで、このカード用パスワードを外側から不正に読み出すことはできず、従って、他人が自分でワンタイム・パスワードを生成して不正使用を行うことは不可能である。

【0075】さらに、通信サーバが利用者の認証と通信端末機120の認証とを同時に行うことができる。

【0076】なお、ICカード100の各格納領域101～103および通信端末機120の各格納領域121、122としては、他人の不正なデータの読み出しを困難にすることができるとな不揮発性メモリを使用することが望ましい。

【0077】

【発明の効果】以上詳細に説明したように、この発明に係る利用者カード、通信端末機、通信サーバ、通信システム、および、通信システムの利用者認証方法によれば、利用者の操作が簡単で、且つ、利用者と通信端末機の認証とを両方同時に行うことができる。

【図面の簡単な説明】

【図1】実施の形態に係る通信システムの全体構成を概念的に示すブロック図である。

【図2】実施の形態に係る利用者カードの内部構成を概念的に示すブロック図である。

【図3】実施の形態に係る通信端末機の内部構成を概念的に示すブロック図である。

【図4】実施の形態に係る通信サーバの内部構成を概念的に示すブロック図である。

【図5】実施の形態で使用するデータの構成を示す概念図である。

【図6】実施の形態で使用するデータの構成を示す概念図である。

【符号の説明】

100 ICカード
101 利用者ID格納領域
102 カード用パスワード格納領域
103 秘密鍵格納領域
104 暗号化機能部
110 カード読み書き機
120 通信端末機
121 端末機ID格納領域
122 端末パスワード格納領域
123 チャレンジ要求機能部
130 通信網
140 通信サーバ
141 シード格納領域
142 秘密鍵格納領域
143 端末機表
144 ICカード表
145 チャレンジ生成機能部
146 カード暗号文検証機能部
147 パスワード検証機能部
148 認証機能部

The diagram shows the internal components of the IC card system 140, enclosed in a dashed box. The components and their interconnections are as follows:

- ICカード表 (IC Card Front)** (144) is connected to the **秘密鍵格納領域 (Secret Key Storage Area)** (142) and the **カード暗号文検証機能部 (Card Cipher Text Verification Function Unit)** (146).
- The **秘密鍵格納領域 (Secret Key Storage Area)** (142) is also connected to the **認証機能部 (Authentication Function Unit)** (148).
- The **カード暗号文検証機能部 (Card Cipher Text Verification Function Unit)** (146) is connected to the **認証機能部 (Authentication Function Unit)** (148).
- The **認証機能部 (Authentication Function Unit)** (148) is connected to the **認証要求機部 (Authentication Request Unit)** (149).
- The **認証機能部 (Authentication Function Unit)** (148) is connected to the **パスワード検証機能部 (Password Verification Function Unit)** (147).
- The **パスワード検証機能部 (Password Verification Function Unit)** (147) is connected to the **チャレンジ生成機能部 (Challenge Generation Function Unit)** (145).
- The **パスワード検証機能部 (Password Verification Function Unit)** (147) is also connected to the **シード格納領域 (Seed Storage Area)** (141).
- The **チャレンジ生成機能部 (Challenge Generation Function Unit)** (145) is connected to the **シード格納領域 (Seed Storage Area)** (141).
- The **チャレンジ生成機能部 (Challenge Generation Function Unit)** (145) is connected to the **チャレンジ要求機部 (Challenge Request Unit)** (150).
- The **シード格納領域 (Seed Storage Area)** (141) is connected to the **シード検証機能部 (Seed Verification Function Unit)** (143).

通信サーバの内部構成図

(51)Int.Cl.⁶
G 0 9 C 1/00
H 0 4 L 9/10
9/32

識別記号
660

FI
G O 6 K 19/00
H O 4 L 9/00

	P
6 2 1 A	
6 7 3 A	
6 7 3 B	
6 7 3 E	